

BOX PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
Washington, D.C. 20231

Case Docket No.: 565



Sir:

Transmitted herewith for filing is the patent application of

Applicant: Mark D. Riggins

Title: Systems and Method for Enabling Secure Access to Services in a Computer Network

Enclosed are:

- ☒ 35 pages of specification, claims and abstract.
- ☒ 10 sheets of ☒ informal ☐ formal drawing(s).
- ☒ A declaration and power of attorney.
- ☒ An assignment transmittal.
- ☒ An assignment of the invention to: RoamPage, Inc.
Please record the assignment and return to the undersigned.
- ☐ A certified copy of a _____ application.
- ☐ An associate power of attorney.
- ☒ A verified statement to establish small entity status under 37 CFR §§ 1.9 and 1.27.
- ☐ PTO Form-1449 and copies of cited art.

The filing fee has been calculated as shown below:

For	(Col. 1) No. Filed	(Col. 2) No. Extra	Small Entity		or	Other Than a Small Entity	
			Rate	Fee		Rate	Fee
Basic Fee				\$385.00			\$770.00
Total Claims	30- 20 = *	10	x \$11 =	\$110.00		x \$22 =	\$
Indep. Claims	4- 3 = *	1	x \$40 =	\$40.00	or	x \$80 =	\$
Multiple Dependent Claims Present <input type="checkbox"/>			+ \$130 =	\$0.00		+ \$260 =	\$
*If the difference in column 1 is less than zero, enter 0 in column 2			Total	\$535.00	or	Total	\$

☐ Please charge my Deposit Account No. 06-0600 the amount of \$____. A duplicate copy of this sheet is enclosed.

☒ A check in the amount of \$575.00 to cover the filing fee ☒ and recording of assignment is enclosed.

☒ The Commissioner is hereby authorized to charge payment of the following fees during the pendency of this application or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is enclosed.

☒ Any additional filing fees required under 37 CFR § 1.16.

☒ Any patent application processing fees under 37 CFR § 1.17.

☐ The issue fee set in 37 CFR § 1.18 at or before mailing of the Notice of Allowance, pursuant to 37 CFR § 1.311(b).

Dated: April 8, 1997

Respectfully submitted,

Marc A. Sockol, Registration No. P-40,823
Carr, DeFilippo & Ferrell LLP
2225 East Bayshore Road, Suite 200
Palo Alto, California 94303
(415) 812-3407

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Mark D. Riggins
SERIAL NO.: Unknown
FILING DATE: April 8, 1997
TITLE: System and Method for Enabling Secure Access to Services
in a Computer Network
EXAMINER: Unknown
GROUP ART UNIT: Unknown
ATTY.DKT.NO.: 565

BOX PATENT APPLICATION
ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

CERTIFICATE OF EXPRESS MAIL

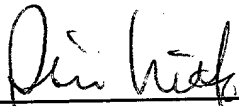
SIR:

"Express Mail" mailing label number EM502168890US

Date of Deposit: April 8, 1997

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Deposited by: Isis E. Nieto


(Signature of person mailing paper or fee)

20250409 095400

10

535.00

201
PATENT

A

SYSTEM AND METHOD FOR ENABLING SECURE ACCESS TO SERVICES IN
A COMPUTER NETWORK

CROSS-REFERENCE TO RELATED APPLICATIONS

5 This application is related to co-pending patent application
entitled "System and Method for Globally Accessing Computer
Services," serial number 08/766,307, filed on December 13, 1996, by
inventors Mark D. Riggins, R. Stanley Bailes, Hong Q. Bui, David J.
Cowan, Daniel J. Mendez, Mason Ng, Sean Michael Quinlan, Prasad
10 Wagle, Christine C. Ying, Christopher R. Zuleeg and Joanna A.
Aptekar-Strober, which subject matter is hereby incorporated by
reference. This related application has been commonly assigned to
RoamPage, Inc.

268040-05671880

15

BACKGROUND OF THE INVENTION

1. Field of the Invention

 This invention relates generally to computer networks, and
more particularly to a system and method for enabling secure access
to services in a computer network.

2. Description of the Background Art

In its infancy, the Internet provided a research-oriented environment where users and hosts were interested in a free and open exchange of information, and where users and hosts mutually
5 trusted one another. However, the Internet has grown dramatically, currently interconnecting about 100,000 computer networks and several million users. Because of its size and openness, the Internet has become a target of data theft, data alteration and other mischief.

Virtually everyone on the Internet is vulnerable. Before
10 connecting, companies balance the rewards of an Internet connection against risks of a security breach. Current security techniques help provide client and server authentication, data confidentiality, system integrity and system access control.

The most popular of the current security techniques is a
15 firewall, which includes an intermediate system positioned between a trusted network and the Internet. The firewall represents an outer perimeter of security for preventing unauthorized communication between the trusted network and the Internet. A firewall may include screening routers, proxy servers and application-layer
20 gateways.

For users on the internet to gain access to protected services on the trusted network, they may be required to provide their identity

to the firewall by some means such as entering a password or by computing a response to a challenge using a hardware token. With proper authentication, the user is allowed to pass through the firewall into the local network, but is typically limited to a
5 predetermined set of services such as e-mail, FTP, etc.

Some local network managers place just outside the firewall a server, often referred to as a "sacrificial lamb" for storing non-confidential data which is easily accessible by the remote user but providing little security.

10 A De-Militarized Zone, or DMZ, sits between two firewalls protecting a trusted network. The external firewall protects servers in the DMZ from external threats while allowing HyperText Transfer Protocol (HTTP) requests. The internal firewall protects the trusted network in the event that one of the servers in the DMZ is
15 compromised. Many companies use DMZs to maintain their web servers.

Another security technique for protecting computer networks is the issuance and use of a public key certificates. Public key certificates are issued to a party by a certificate authority, which via
20 some method validates the party's identity and issues a certificate stating the party's name and public key. As evidence of authenticity,

the certificate authority digitally signs the party's certificate using the certificate authority's private key.

Thus, when a user via a client computer connects to a server, the client computer and server exchange public key certificates.

5 Each party verifies the authenticity of the received certificates by using the certificate authority's public key to verify the signature of the certificate. Then, by encrypting messages with the server's public key the user can send secure communications to the server, and by encrypting messages with the user's public key the server
10 can send secure communications to the user. Although any party might present a public key certificate, only the real user and the real host have the corresponding private key needed to decrypt the message. Examples of authentication and key distribution computer security systems include the KerberosTM security system developed
15 by the Massachusetts Institute of Technology and the NetSPTM security system developed by the IBM Corporation.

These security techniques do not solve problems associated with the roaming (traveling) user. For the roaming user, maintaining identification and authentication information such as passwords,
20 certificates, keys, etc. is a cumbersome process. Further, accessing multiple systems requires multiple keys, which often are too complex to track and use. Also, direct access to systems behind

firewalls compromises security. Therefore, a system and method are needed to enable remote access to computer services easily and securely.

5

SUMMARY OF THE INVENTION

The present invention provides a system and method for enabling secure access to services in a computer network. The network system includes a global server coupled via a computer network to computer services. The global server includes a communications engine for establishing a communications link with a client; security means coupled to the communications engine for determining client privileges; a servlet host engine coupled to the security means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and a key-
safe for storing keys which enable access to the secured services. The global server may be coupled to multiple sites, wherein each site provides multiple services. Each site may be protected by a firewall. Accordingly, the global server stores the keys for enabling communication via the firewalls with the services.

20

The method includes the steps of establishing a communications link with a client; identifying and authenticating the client; determining client privileges; providing to the client, based on

the client privileges, an applet which enables I/O with a secured service; and retrieving a key which enables access to the secured service.

The system and method of the present invention
5 advantageously provide a globally-accessible trusted third party, i.e.,
the global server. This trusted third party securely stores keys, and
acts as a single identification and authentication service. Other
systems may be accessed through the global server. The global
server uses the stored keys to authenticate the user under an
10 identity that is understood by the other system's existing security
services, and establishes a secure communications channel to the
desired service. Because of a global firewall, the global server is
substantially protected from external threats. Accordingly, the
global server provides authorized clients with secure communication
15 through firewalls with services. The global server may enable
multiple levels of identification and authentication services.
Accordingly, the global server may enable multiple levels of resource
access based on the user's status, the strengths of the identification
and the authentication and on the privacy of the communications
20 channel.

Because of the global firewall and the identification and
authentication services performed by the global server, corporations

can store relatively secret information on the global server for use
by authorized clients. Yet, the present invention also enables
corporations to maintain only a portion of their secret information on
the global server, so that there would be only this limited loss should
5 the trusted third party system be compromised. Further, the global
server advantageously may act as a client proxy for controlling
access to services, logging use of keys and logging access of resources.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram illustrating a roaming-user network access system, in accordance with the present invention;

FIG. 2 is a block diagram illustrating details of an example
5 client of FIG. 1;

FIG. 3 is a block diagram illustrating details of the global server of FIG. 1;

FIG. 4 is a block diagram illustrating details of an example service server of FIG. 1;

10 FIG. 5 is a flowchart illustrating a method for remotely accessing a secure service;

FIG. 6 is a flowchart illustrating details of the FIG. 5 step of creating a link between a client and the global server of;

FIG. 7 illustrates an example web page;

15 FIG. 8A is a flowchart illustrating details of the FIG. 5 step of accessing a service in a first embodiment;

FIG. 8b is a flowchart illustrating details of the FIG. 5 step of accessing a service in a second embodiment; and

FIG. 8C is a flowchart illustrating details of the FIG. 5 step of
20 accessing a service in a third embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating an exemplary roaming-user network access system 100 in accordance with the present invention. System 100 includes an interconnected network of computers referred to herein as an "Internet" 102. System 100 further includes a first company network 112, a second company network 118, a kiosk network 138 and an Internet Service Provider (ISP) network 143, each network being coupled to the Internet 102.

Company network 112 includes a firewall 116 coupled between the Internet 102 and a client computer 114a. Company network 118 includes a firewall 120 coupled between the Internet 102 and an internal network signal bus 126. Company network 118 further includes a first server 108a for providing a first service 110a, a second server 108b for providing a second service 110b, a first client computer 114b storing a program for providing a third service 110c and a second client computer 114c, each being coupled to signal bus 126. Example services 110a-110d include an e-mail service program, an address book service program, a calendar service program, a paging service program, and a company database service program.

The kiosk network 138 includes a first client computer 114d and a second client computer 114e, each being coupled to the

Internet 102. The ISP network 143 includes an ISP 148 coupled via a wireless channel 146 to a first client computer 114f and coupled via modems 152 and 156 and via transmission line 154 to a second client computer 114g.

5 The Internet 102 includes a global server 106 which is protected by a global firewall 104 and includes a server 108c for providing a service 110d. Intercommunication between client computers 114a-114g and services 110a-110d is accomplished via the global server 106. If, for example, a user of any one of the client
10 computers 114a-114g wants to access a service 110a-110d (which is provided at a location within system 100 that is unknown to the user), then the user applies a known Uniform Resource Locator (URL) to access a web page operated by global server 106. An example web page 700 is shown in and described with reference to FIG. 7.
15 The global firewall 104 protects the global server 106 from external threats.

Before obtaining access privileges to the functionality provided by the global server 106, the user must first obtain authorization from the global server 106. Obtaining authorization typically
20 requires user identification and authentication, for example, using public-key certificates. Once authenticated, the global server 106 provides the user with access to the services 110a-110d. It will be

appreciated that varying levels of access to services 110a-110d will be granted based on varying strengths of identification and authentication and on the privacy of the communications channel.

To enable user access to and control of the services 110a-110d, the global server 106 may use conventional applets, servlets or agents in a distributed network environment, such as the JavaTM distributed environment produced by the Netscape Corporation. The global server 106 provides the user's client with access to and control of the service 110a-110d. The global server 106 may redirect the user's client to access the service 110a-110d itself, the global server 106 may access the service 110a-110d itself and provide I/O to the client by proxy, or the global server 106 may provide the service 110a-110d itself. These three different modes of access to the services 110a-110d are described with reference to FIGs. 8A-8C.

The global server 106 maintains the network addresses of all the services 110a-110d, the user's public and private keys, the user's account numbers, firewall authentication information, etc. Firewall authentication information includes the necessary identification, passwords and certificates needed to pass firewalls 116 and 120. Accordingly, the user need only maintain the URL of the global server 106, and identification and authentication information such as

a password or hardware token for obtaining access to the functionality of the global server 106. Thus, the roaming user can access computer services 110a-110d using any computer terminal which is connected to the Internet 102.

5

FIG. 2 is a block diagram illustrating details of a client computer 114, such that each of clients 114a-114d is an instance of the client 114. The client 114 includes a Central Processing Unit (CPU) 210 such as a Motorola Power PC[®] microprocessor or an Intel Pentium[®] microprocessor. An input device 220 such as a keyboard and mouse, and an output device 230 such as a Cathode Ray Tube (CRT) display are coupled via a signal bus 240 to CPU 210. A communications interface 250, a data storage device 260 such as Read Only Memory (ROM) or a magnetic disk, and a Random-Access Memory (RAM) 270 are further coupled via signal bus 240 to CPU 210. The communications interface 250 of client computer 114 is coupled to the Internet 102 as shown in and described with reference to FIG. 1.

An operating system 280 includes a program for controlling processing by CPU 210, and is typically stored in data storage device 260 and loaded into RAM 270 for execution. Operating system 280 includes a communication engine 282 for generating and transferring

message packets to and from the internet 106 via the communications interface 250.

Operating system 280 further includes an internet engine such as a web browser 284, e.g., the Netscape™ web browser produced by the Netscape Corporation or the Internet Explorer™ web browser produced by the Microsoft Corporation. The web browser 284 includes an encryption engine 285 for encrypting messages using public and private keys, and an applet engine 286 for executing applets 288 downloaded from the global server 106 to enable the access to computer services 110a-110d. Downloaded applets 288 may include security applets 290 for performing services such as user identification and authentication, message integrity services, and certificate verification. The browser 284 further receives web page data (391, FIG. 3), configuration data 390 and information identifying a set of selectable services 110a-110d, and uses the information to display the web page (700, FIG. 7). The web browser 284 enables a user via the client 114a-114g to select one of the services 110a-110d for execution.

It will be appreciated that a client 114a-114g such as client 114b may include a service engine 490 (see FIG. 4) for providing a service 110a-110d such as service 110c. Thus, it is possible for a client 114b user to request access to service 110c via the global

server 106, without knowing that the service 110c is provided by client 114b. Accordingly, the global server 106 will provide client 114 with an applet 288 for providing user interface I/O of service 110c back to client 114b.

5

FIG. 3 is a block diagram illustrating details of the global server 106, which includes a CPU 310 such as a Motorola Power PC[®] microprocessor or an Intel Pentium[®] microprocessor. An input device 320 such as a keyboard and mouse, and an output device 330 such as a CRT display are coupled via a signal bus 340 to CPU 310. A communications interface 350, a data storage device 360 such as ROM or a magnetic disk, and a RAM 370 are further coupled via signal bus 340 to CPU 310. The communications interface 350 is conventionally coupled as part of the Internet 102 to the clients 114. Although the global server 106 is described as a single computer, it will be appreciated that the global server 106 may include multiple computers networked together.

Operating system 380 includes a program for controlling processing by CPU 310, and is typically stored in data storage device 260 and loaded into RAM 370 for execution. Operating system 380 includes a communication engine 382 for generating and transferring

message packets to and from client computers 114 via the communications interface 350.

Operating system 380 further includes, as part of global firewall 104, security services 384 for opening a communications channel with users. For example, when a client attempts to access the global server 106, the security services 384 first determines whether the global server 106 accepts in-bound communications from a particular port (not shown) and whether the servlet host engine 386, described below, is authorized to connect to that particular port. If so, the security services 384 allows the communications engine 382 to open a communications channel via the particular port to the client 114a-114g. Otherwise, no channel will be opened.

The operating system 380 further includes a web engine 387 which, based on user's identification, the strength of the user's authentication and the privacy of the communications channel, forwards web page data 391 and information identifying a set of available services 110a-110d to the client 114a-114g. An example web page 700 is shown and described with reference to FIG. 7. The web engine 387 enables a user to select a service 110a-110d from the web page 700.

The web engine 387 includes a servlet host engine 286, which downloads security applets 290 including an authentication applet (not shown) to the client computer 114 and accordingly executes an authentication servlet 397 of servlets 398 for performing

5 identification and authentication services. The authentication applet 290 prompts the user for identification and authentication information, and then communicates the information to the authentication servlet 397. The authentication servlet 397 verifies that the information is correct. It will be noted that the user's
10 authentication information is not necessarily sent to the authentication servlet 397, but rather its existence and correctness is proven via a secure means such as a secure hash. The servlet host engine 386 further includes a secure communications engine 396 which may use public key certificates to negotiate a secure
15 communications channel with the client computer 114.

Upon selection of a service 110a-110d, the servlet host engine 386 downloads a corresponding applet 388, corresponding configuration data 390 and corresponding user data 392 and may download corresponding service address information 394 to the
20 client computer 114. Configuration data 390 includes information for configuring the user's web browser 284, for configuring the downloaded applets 288, and for configuring the selected service

110a-110d. Configuration is described in the related co-pending application referenced above. User data 392 may include user-and-service-specific information such as stored bookmarks, calendar data, pager numbers, etc. which was specifically stored on the global

5 server 106 for easy access. Service address information 394 identifies the location of the services 110a-110d provided in system 100 by the global server 106. The client computer 114 executes the corresponding downloaded applet 288, which via the servlet host engine 386 (possibly using a corresponding servlet 398) enables the
10 user to access and to control the corresponding services 110a-110d. The downloadable applets 388, configuration data 390, user data 392 and service address information 394 may be stored on the data storage device 360.

A key safe 395 is a data file for storing each user's
15 identification information, each user's public and private keys, each firewall's password information, etc. The key safe 395 is organized in a linked list format so that, based on the selected service 110a-110d, the global server 106 can retrieve the appropriate firewall's password information, the appropriate user's identification
20 information and keys, etc. The key safe 395 may be stored on the data storage device 360.

FIG. 4 is a block diagram illustrating details of a service server 108, such that servers 108a-108c and client 114b are instances of server 108. Server 108 includes a CPU 410 such as a Motorola Power PC[®] microprocessor or an Intel Pentium[®] microprocessor. An input device 420 such as a keyboard and mouse, and an output device 430 such as a CRT display are coupled via a signal bus 440 to CPU 410. A communications interface 450, a data storage device 460 such as ROM or a magnetic disk, and a RAM 470 are further coupled via signal bus 440 to CPU 410. The communications interface 450 is coupled to the clients 114 as shown in and described with reference to FIG. 1.

The operating system 480 includes a program for controlling processing by CPU 410, and is typically stored in data storage device 460 and loaded into RAM 470 for execution. Operating system 480 also includes a communications engine 482 for generating and transferring message packets via the communications interface 450 to and from clients 114 or to and from global server 106. Operating system 480 further includes security services 484 for negotiating a secure channel with users, a secure communications engine 486 for opening the secure channel with the users, and a service engine 490 for providing a service 110a-110d to the users.

The service engine 490 includes a service interface 492 for receiving and translating messages to and from downloaded applets 288 currently executing on the client 114, and includes a service processor 494 and service data 496 for processing the service requests from the user. The service data 496 may include previously-generated documents, database information, etc. It will be appreciated that the service data 496 is similar to the user data 392, such that it includes the same type of information but is maintained on the service server 108 instead of on the global server 108.

FIG. 5 is a flowchart illustrating a method 500 enabling a user to access services 110a-110d in computer network system 100. Method 500 begins by the client 114 in step 505 creating a communications link with the global server 106. Step 505 is described in greater detail with reference to FIG. 6. The global server 106 in step 510 confirms that the user has privileges to access the functionality of the global server 106. Confirming user access privileges may include examining a user certificate, obtaining a secret password, using digital signature technology, etc. It will be appreciated that the security services 384 may cause the servlet host

engine 386 to forward a security applet 389 via the communications channel to the client 114 for performing user authentication.

After user access privileges are confirmed, the web page engine 387 of the global server 106 in step 515 downloads web page data 391 and configuration data 390 to the client 114. The browser 284 of the client 114 in step 520 uses the web page data 391 and the configuration data 390 to display a web page 700 (FIG. 7) on the output device 230 of the client 114 and to enable access to the services 110a-110d which are offered by the global server 106. An example web page 700 is shown and described with reference to FIG. 7. Configuration of the client 114 and of the web page 700 are described in detail in the cross-referenced patent application.

From the options listed on the web page 700, the user in step 525 via input device 220 selects a service 110a-110d. In response, the servlet host engine 386 of the global server 106 in step 530 downloads the corresponding applet(s) 388, applet configuration data 390, user data 392 and possibly service address information 394 to the client 114. Applet configuration data 390 preferably includes user-specific preferences, such as user-preferred fonts, for configuring the selected service 110a-110d. User data 392 may include user-specific and service-specific information such as stored bookmarks, calendar data, pager numbers, etc. Service address

information 394 identifies the location of the selected service 110a-110d. Alternatively, the corresponding applet(s) 388, applet configuration data 390, user data 392 and service address information 394 could have been downloaded in step 515 with the
5 web page data 391 and the configuration data 390.

The applet engine 286 of the client 114 in step 535 executes the corresponding downloaded applet 288. The service server 108 in step 537 initiates the service engine 490. The global server 106 in step 538 selects one of the three modes of access described in FIGs. 8A-8C for enabling the client computer 114 to communicate with the
10 corresponding service engine 490. For example, if the user selects the service 110d on server 108c, which is not protected by a separate firewall, then the global server 106 may provide the user with direct access. If the user selects service 110a provided by
15 server 108a within company network 118, then the global server 106 may access the service 110a as a proxy for the user. It will be appreciated that each firewall 106 and 120 may store policies establishing the proper mode of access the global server 106 should select. Other factors for selecting mode of access may include user
20 preference, availability and feasibility. The global server 106 in step 540 provides the client 114 user with access to the selected service

110a-110d. Step 540 is described in greater detail with reference to FIGs. 8A, 8B and 8C.

FIG. 6 is a flowchart illustrating details of step 505, which
5 begins by the client 114 user in step 605 using a known Uniform
Resource Locator (URL) to call the global server 106. The global
server 106 and the client 114 in step 607 create a secure
communications channel therebetween, possibly by applying Secure
Sockets Layer (SSL) technology. That is, the security services 384 of
10 the global server 106 in step 610 determine if in-bound secure
communications are permitted and, if so, creates a communications
channel with the client 114. The browser 284 of the client 114 and
the security services 384 of the global server 106 in step 615
negotiate secure communications channel parameters, possibly using
15 public key certificates. An example secure communications channel
is RSA with RC4 encryption. It will be appreciated that the global
server 106 may be configured to use one of ten encryption protocols
and the client 114 may be enabled to use one of five encryption
protocols. Step 615 thus may include selecting one of the encryption
20 protocols which is common to both the global server 106 and the
client 114. The encryption engine 285 of the client 114 and secure
communications engine 396 of the global server 114 in step 620 use

the secure channel parameters to create the secure communications channel. Method 505 then ends.

FIG. 7 illustrates an example URL-addressable HyperText

5 Markup Language (HTML)-based web page 700, as maintained by the servlet host engine 386. The web page 700 includes a title 710 "Web Page," a listing of the provided services 715 and a pointer 770 for selecting one of the provided services 715. As illustrated, the provided services 715 may include an e-mail service 720, a
10 calendaring service 730, an internet access service 740, a paging service 750 and a fax sending service 760. Although not shown, other services such as bookmarking, QuickCard™, etc. may be included in the web page 700.

15 FIG. 8A is a flowchart illustrating details of step 540 in a first embodiment, referred to as step 540a, wherein the global server 106 provides the client 114 with a direct connection to the service 110a-110d. Step 540a begins by the downloaded applet 288 in step 805 retrieving the service address 394 of the selected service 110a-110d
20 from data storage device 360 and the authentication information for the service 110a-110d from the key safe 395. The communications engine 282 in step 810 creates a direct and secure connection with

the communications engine 482 of the service server 108 at the
retrieved service address, and uses the authentication information to
authenticate itself. The applet 288 in step 815 acts as the I/O
interface with the service engine 490, which is described in detail in
5 the cross-referenced patent application. Step 540a then ends.

FIG. 8B is a flowchart illustrating details of step 540 in a second
embodiment, referred to as step 540b, wherein the global server 106
acts for the client 114 as a proxy to the service 110a-110d. Step
10 540b begins with the applet 288 in step 840 retrieving the "service"
address, which results in directing it to the global server 106. Thus,
the applet 288 in step 845 creates a connection with the global
server 106. The servlet host engine 386 of the global server 106 in
step 850 retrieves the service address of the selected service 110a-
15 110d and the authentication information for the selected service
110a-110d from the keystore 395. The secure communications
engine 396 of the global server 106 in step 855 negotiate secure
channel parameters for creating a secure channel with the secure
communications engine 486 of the service server 108.

20 Thereafter, the applet 288 in step 860 acts as the I/O interface
(enables the user to make requests of the service engine 490) with
the secure communications engine 396 of the global server 106. If

the servlet host engine 386 in step 865 determines that it is unauthorized to perform a client 114 user's request, then the servlet host engine 386 in step 870 determines whether the method 540b ends, e.g., whether the user has quit. If so, then method 820b ends.

5 Otherwise, method 540b returns to step 860 to obtain another request. If the servlet host engine 386 in step 865 determines that it is authorized to perform the client 114 user's request, then the servlet host engine 386, possibly using servlets 398, acts as the proxy for the client 114 to the service engine 490. As proxy, the
10 servlet host engine 386 forwards the service request to the service 110a-110d for the applet 288 and forwards responses to the requesting applet 288 currently executing on the client 114. Method 540b then returns to step 870.

15 FIG. 8C is a flowchart illustrating details of step 540 in a third embodiment, referred to as step 540c, wherein the service 110a-110d being requested is located on the global server 106. Step 540c begins with the applet 288 in step 880 retrieving the service address for the service 110a-110d, which results in providing the applet 288
20 with the service address of the service 110a-110d on the global server 106. Thus, the applet 288 in step 882 creates a secure connection with the global server 106. No additional step of

identification and authentication is needed since the client 114 has already identified and authenticated itself to the global server 106 in step 510 of FIG. 5.

In step 884, a determination is made whether the service 110a-110d is currently running. If so, then in step 886 a determination is made whether the service 110a-110d can handle multiple users. If not, then the global server 106 in step 890 creates an instance for the user, and the applet 288 in step 892 acts as the I/O interface with the service 110a-110d on the global server 106. Otherwise, if the service 110a-110d in step 886 determines that it cannot handle multiple users, then method 540a proceeds to step 892. Further, if in step 884 the global server 106 determines that the service 110a-110d is not currently running, then the global server 106 in step 888 initializes the service 110a-110d and proceeds to step 886.

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of

interconnected conventional components and circuits. The
embodiments described herein have been presented for purposes of
illustration and are not intended to be exhaustive or limiting. Many
variations and modifications are possible in light of the foregoing
5 teaching. The invention is limited only by the following claims.

WHAT IS CLAIMED IS:

1 1. A system comprising:
2 a communications engine for establishing a communications
3 link with a client;
4 security means coupled to the communications engine for
5 determining client privileges;
6 a servlet host engine coupled to the security means for
7 providing to the client, based on the client privileges, an applet
8 which enables I/O with a secured service; and
9 a key safe for storing a key which enables access to the secured
10 service.

1 2. The system of claim 1, wherein the communications engine
2 uses SSL technology to create a secure communications link with the
3 client.

1 3. The system of claim 1, wherein communications engine
2 negotiates an encryption protocol for transferring messages to and
3 from the client.

1 4. The system of claim 1, wherein the communications engine
2 uses public key certificates for transferring messages to and from the
3 client.

1 5. The system of claim 1, wherein the security means uses public
2 key certificates to authenticate the client.

1 6. The system of claim 1, wherein the security means examines
2 client identity and the level of authentication to determine client
3 privileges.

1 7. The system of claim 1, wherein the security means examines a
2 global certificate to authenticate the client.

1 8. The system of claim 1, wherein the security means uses digital
2 signature technology to authenticate the client.

1 9. The system of claim 1, wherein the servlet host engine
2 forwards to the client a security applet for enabling the client to
3 perform a security protocol recognized by the security means.

1 10. The system of claim 1, wherein the service is secured by a
2 corporate firewall and the key is configured to enable communication
3 through the firewall.

1 11. The system of claim 1, further comprising a global firewall for
2 protecting the system.

1 12. The system of claim 1, further comprising a service address for
2 identifying the location of the secured service.

1 13. The system of claim 1, wherein the applet provides to the
2 client a direct connection with the secured service.

1 14. The system of claim 1, further comprising a proxy in
2 communication with the secured service, and wherein the applet
3 enables I/O with the proxy.

1 15. A method comprising the steps of:
2 establishing a communications link with a client;
3 determining client privileges;
4 providing to the client, based on the client privileges, an applet
5 which enables I/O with a secured service; and
6 retrieving a key which enables access to the secured service.

1 16. The method of claim 15, wherein establishing a
2 communications link includes the step of using SSL technology to
3 create a secure communications link with the client.

1 17. The method of claim 15, wherein establishing a
2 communications link includes the step of negotiating an encryption
3 protocol for transferring messages to and from the client.

1 18. The method of claim 15, wherein establishing a
2 communications link includes the step of using public key certificates
3 for transferring messages to and from the client.

1 19. The method of claim 15, wherein determining client privileges
2 includes the step of using public key certificates to authenticate the
3 client.

1 20. The method of claim 15, wherein determining client privileges
2 includes the step of examining client identity and the level of
3 authentication to determine client privileges.

1 21. The method of claim 15, wherein determining client privileges
2 includes the step of examining a global certificate to authenticate the
3 client.

1 22. The method of claim 15, wherein determining client privileges
2 includes the step of using digital signature technology to authenticate
3 the client.

1 23. The method of claim 15, wherein establishing a
2 communications link includes forwarding to the client a security
3 applet for enabling the client to perform a recognized security
4 protocol.

1 24. The method of claim 15, further comprising the step of using
2 the key to communicate through a firewall to the secured service.

1 25. The method of claim 15, wherein the method is performed by a
2 global server and further comprising using a global firewall to
3 protect the global server.

1 26. The method of claim 15, further comprising using a service
2 address to identify the location of the secured service.

1 27. The method of claim 15, wherein providing includes the step of
2 providing to the client a direct connection with the secured service.

1 28. The method of claim 15, further comprising using a proxy in
2 communication with the secured service, and wherein providing
3 includes enabling I/O with the proxy.

1 29. A system comprising:
2 means for establishing a communications link with a client;
3 means for determining client privileges;
4 means for providing to the client, based on the client privileges,
5 an applet which enables I/O with a secured service; and
6 means for retrieving a key which enables access to the secured
7 service.

1 30. A computer-based storage medium storing a program for
2 causing a computer to perform the steps of:
3 establishing a communications link with a client;
4 determining client privileges;
5 providing to the client, based on the client privileges, an applet
6 which enables I/O with a secured service; and
7 retrieving a key which enables access to the secured service.

SYSTEM AND METHOD FOR ENABLING SECURE ACCESS TO SERVICES IN
A COMPUTER NETWORK

ABSTRACT OF THE DISCLOSURE

5

268040 0567880
450450 040897

A global server includes a communications engine for establishing a communications link with a client; security means coupled to the communications engine for determining client privileges; a servlet host engine coupled to the security means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and a key safe for storing a key which enables access to the secured service. The global server may be coupled to multiple sites, wherein each site provides multiple services. Each site may be protected by a firewall. Accordingly, the global server stores the keys for enabling communication via the firewalls with the services.

10
15

FIG. 100

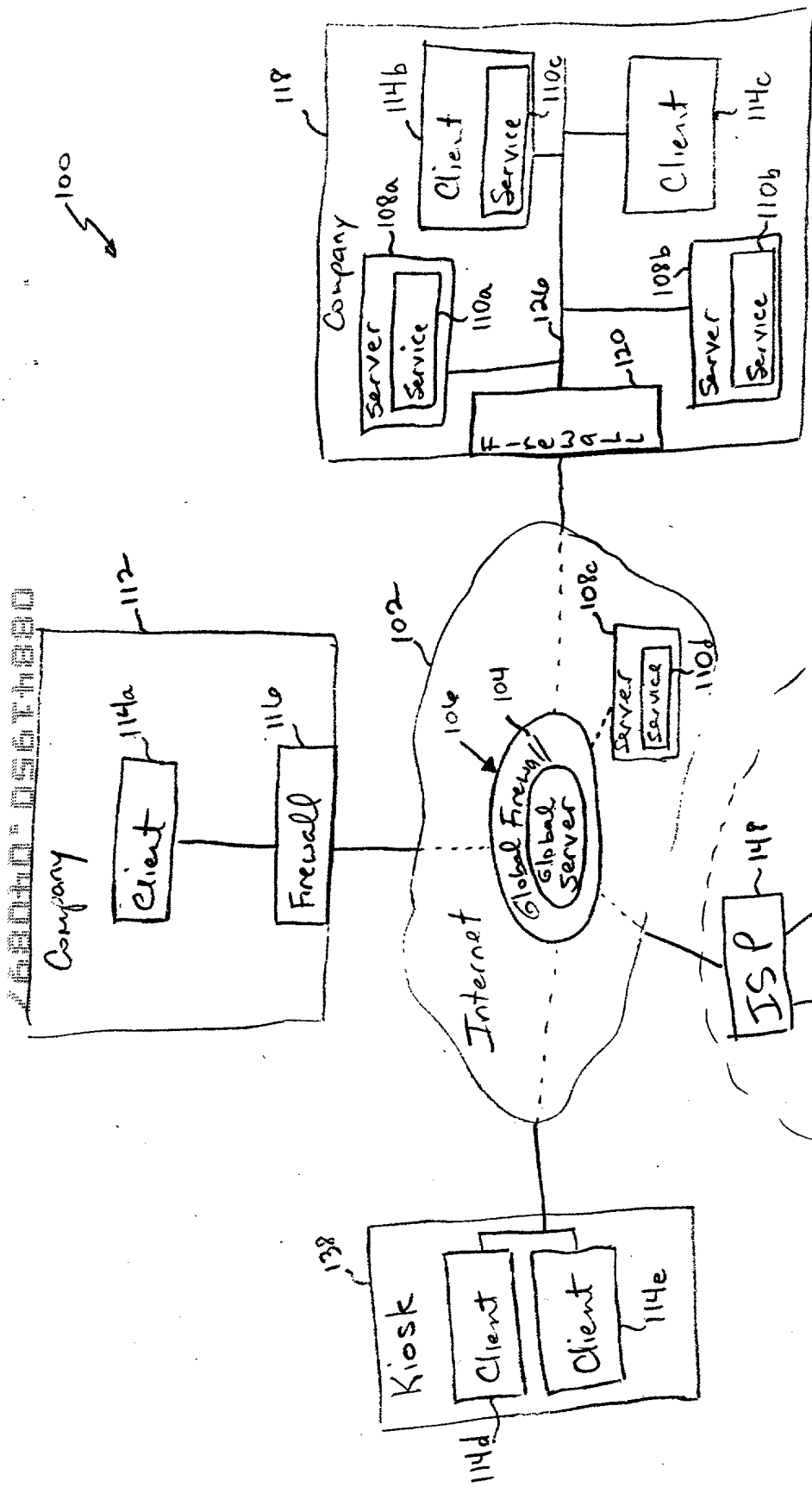
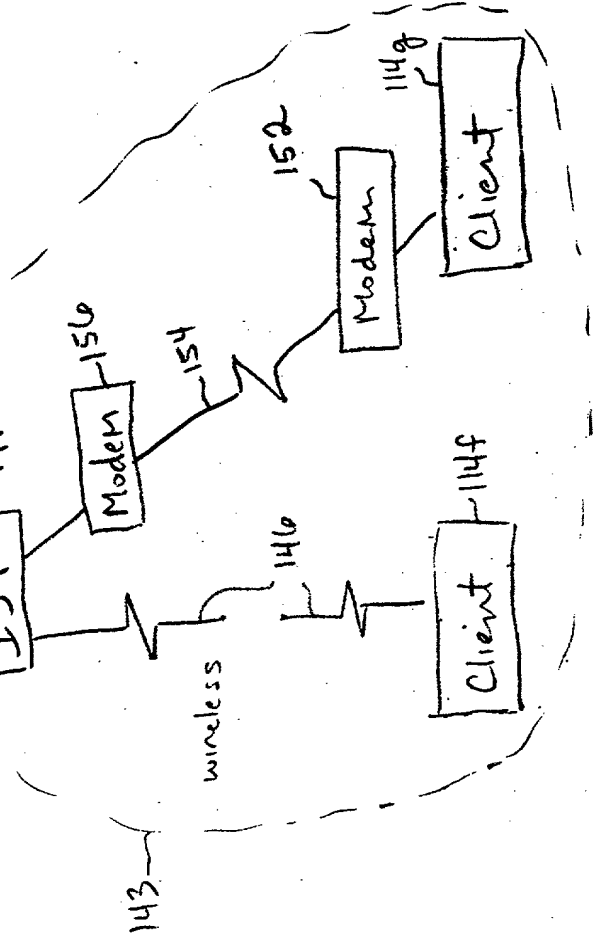


FIG. 1

(Roaming Internet Access System)



Client 114

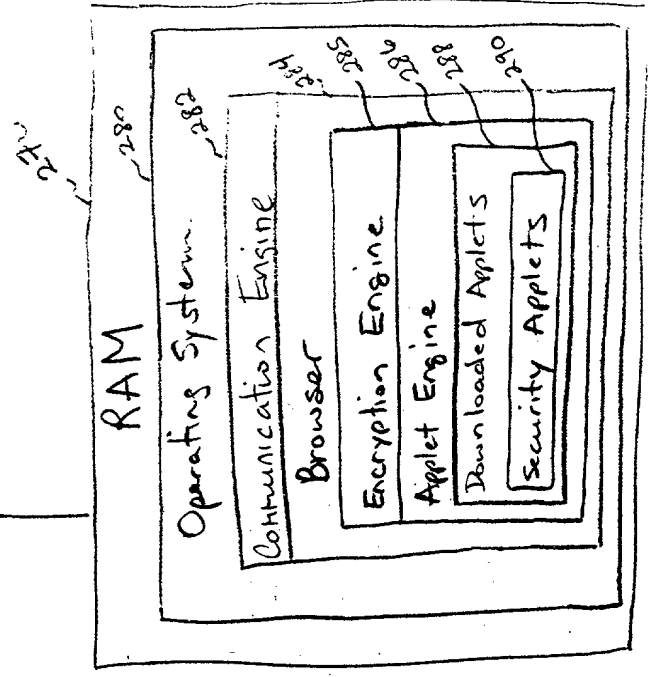
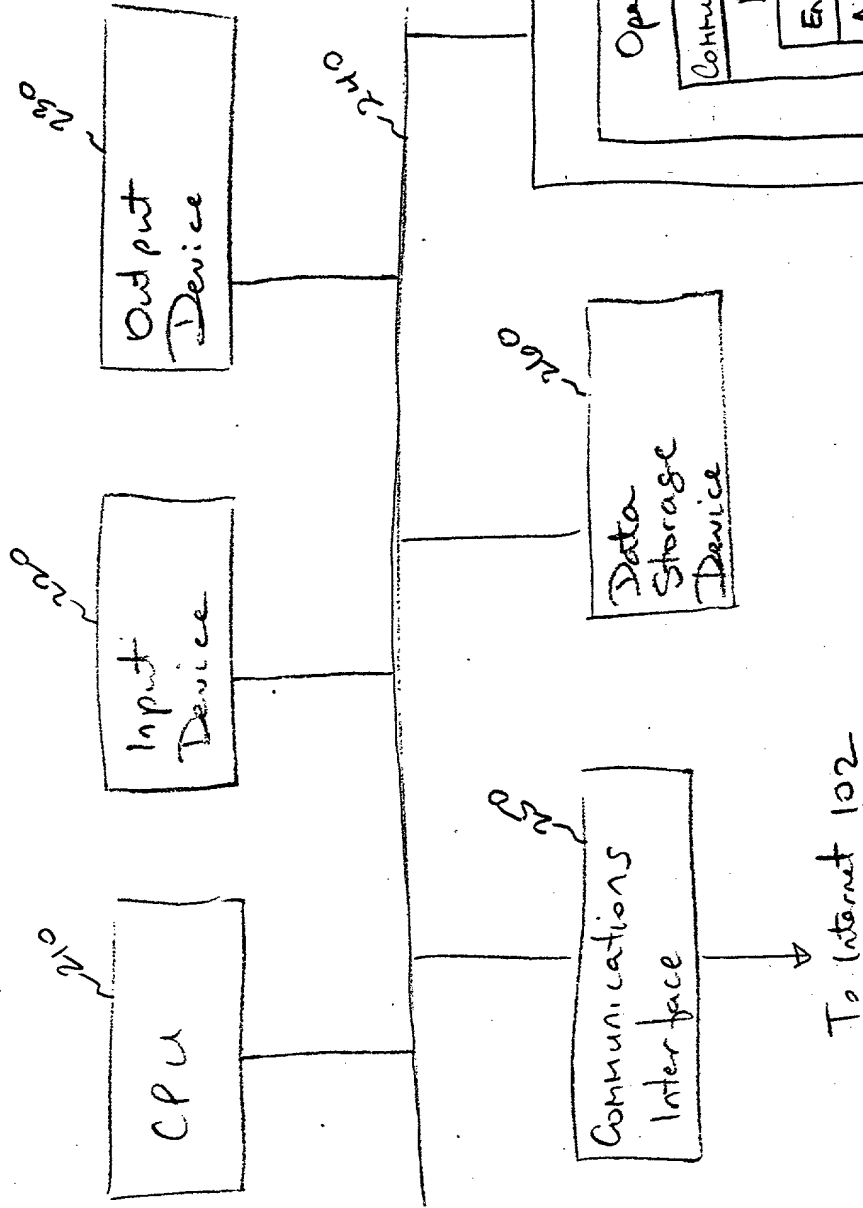


FIG. 2

Global
Server
106

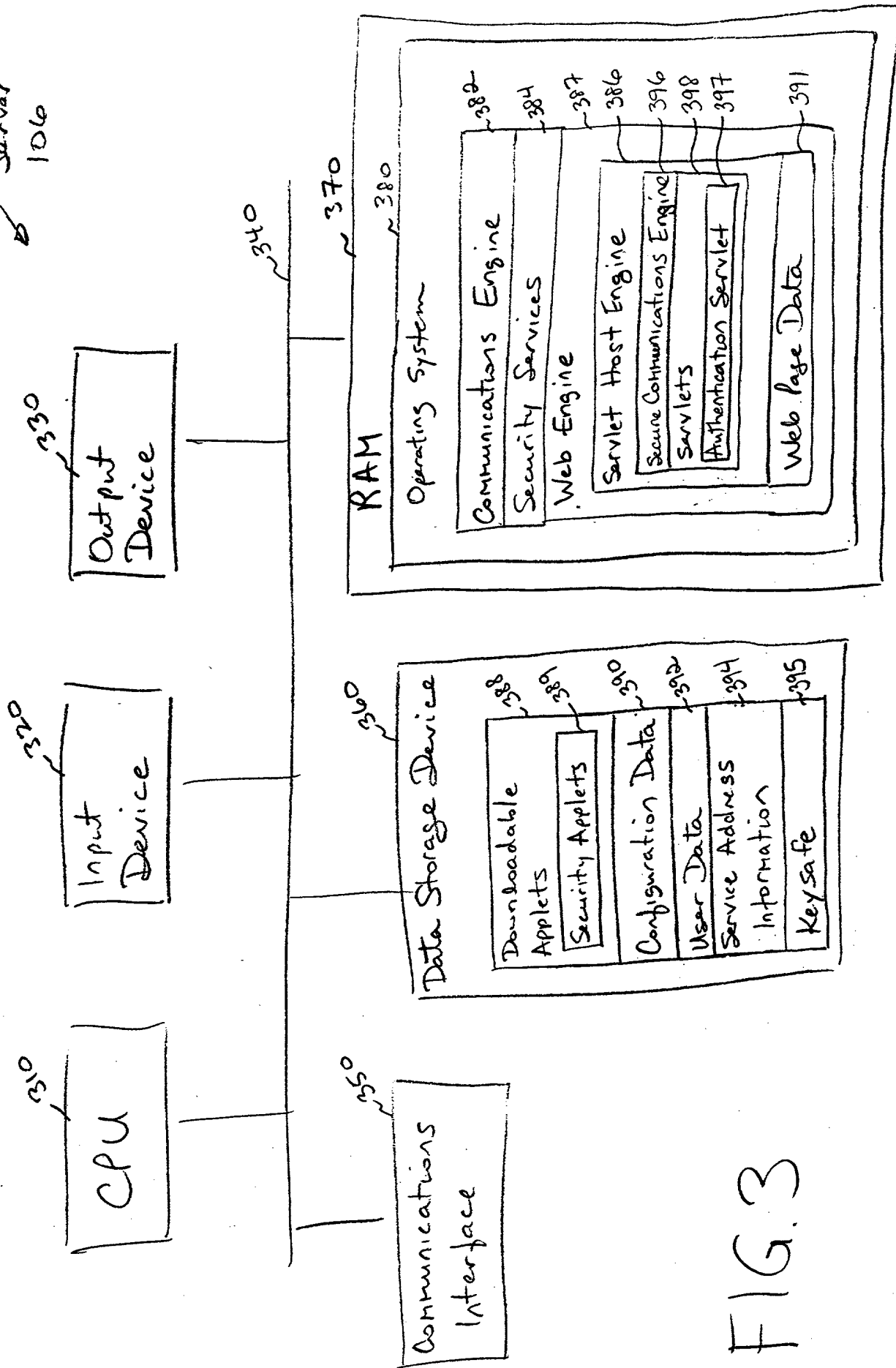


FIG. 3

Service
Server
108

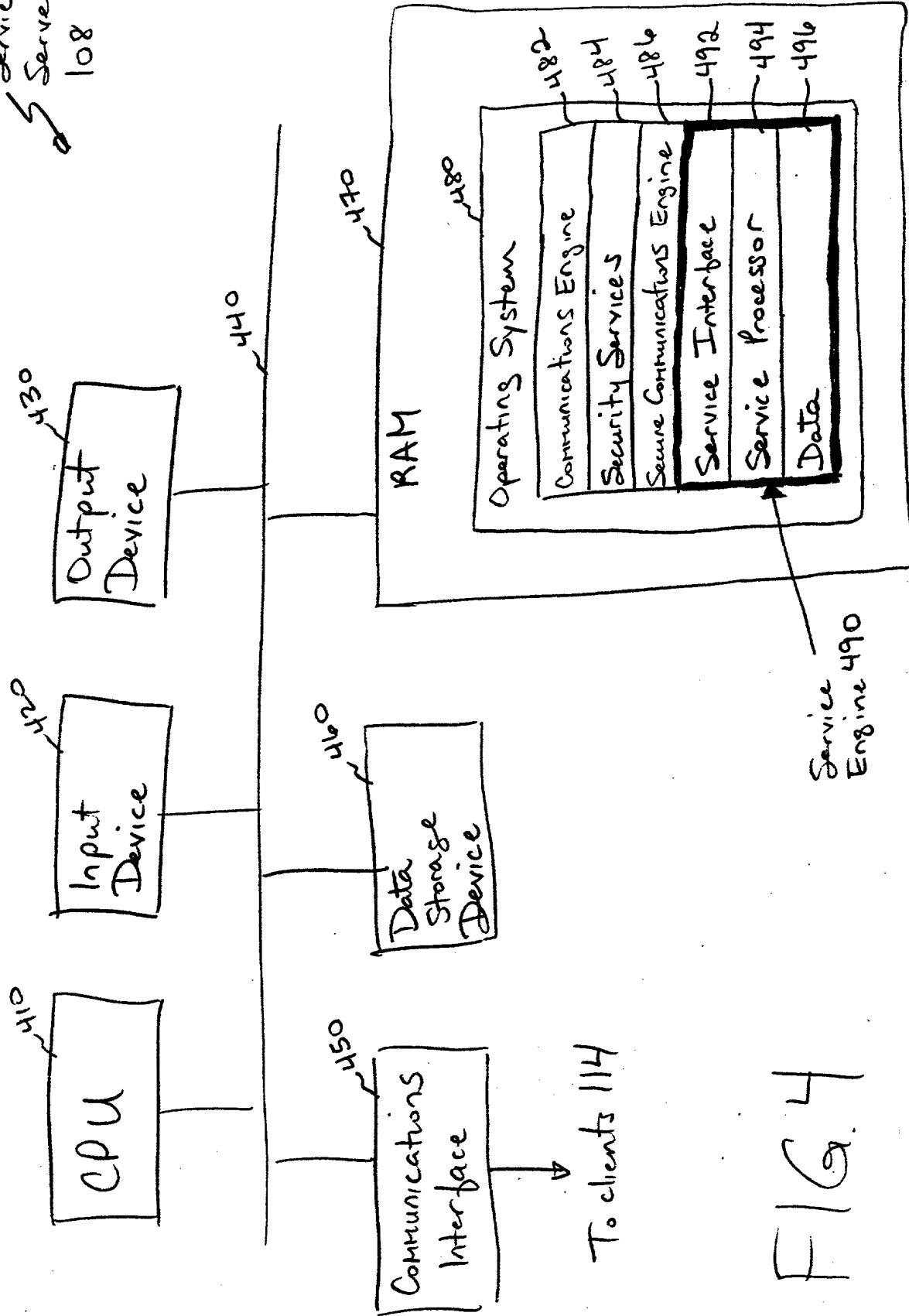


FIG. 4

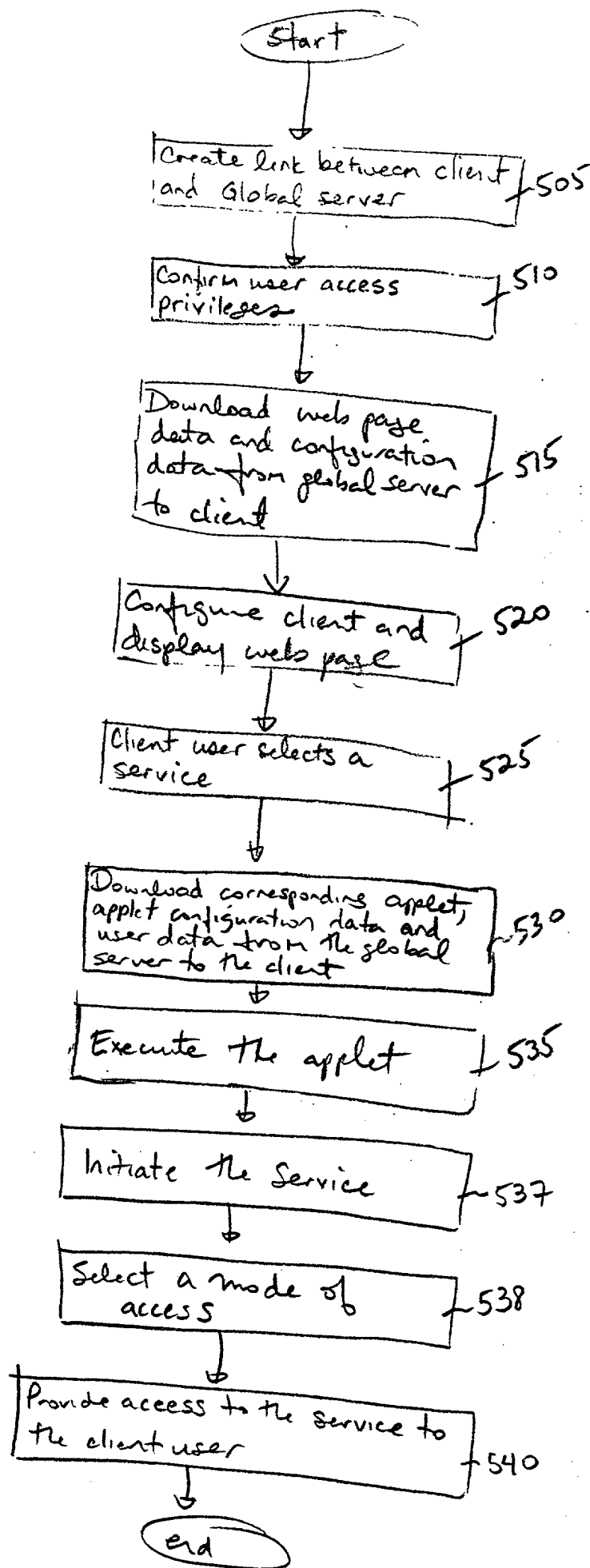


FIG. 5

20240404 05:00:00

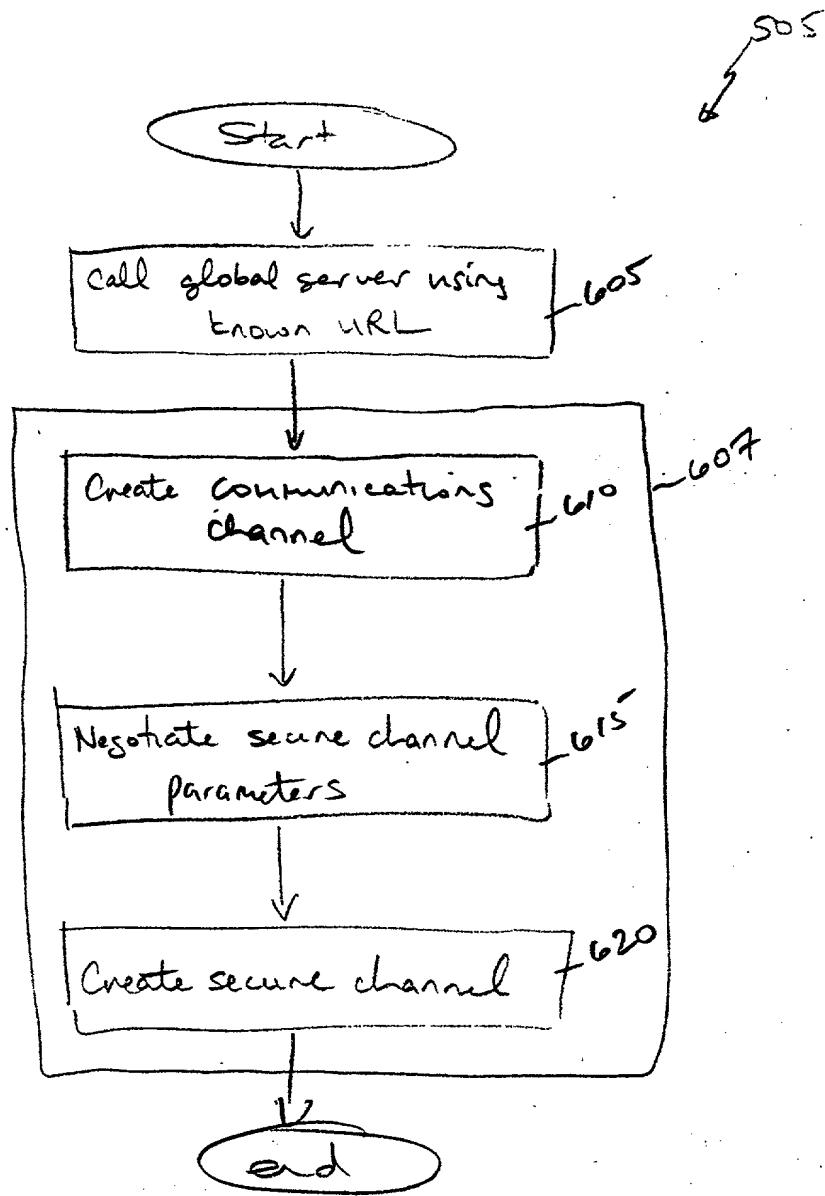


FIG. 6

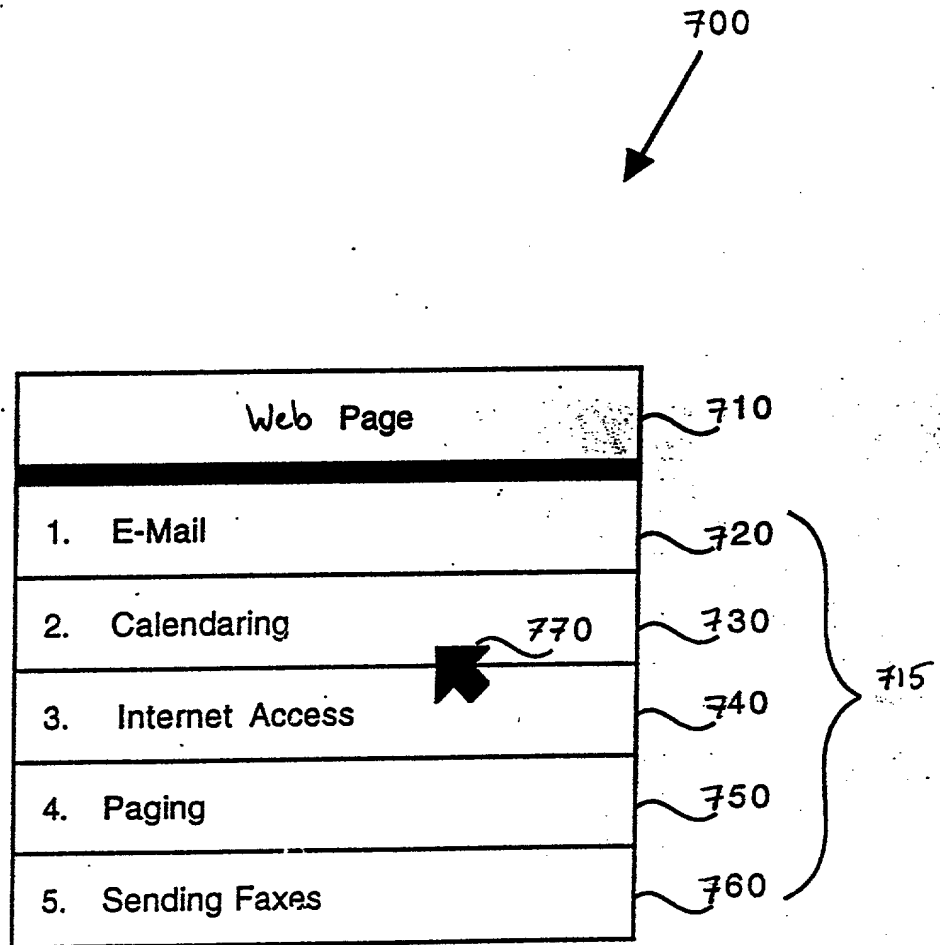


FIG. 7
(Web Page Screen Shot)

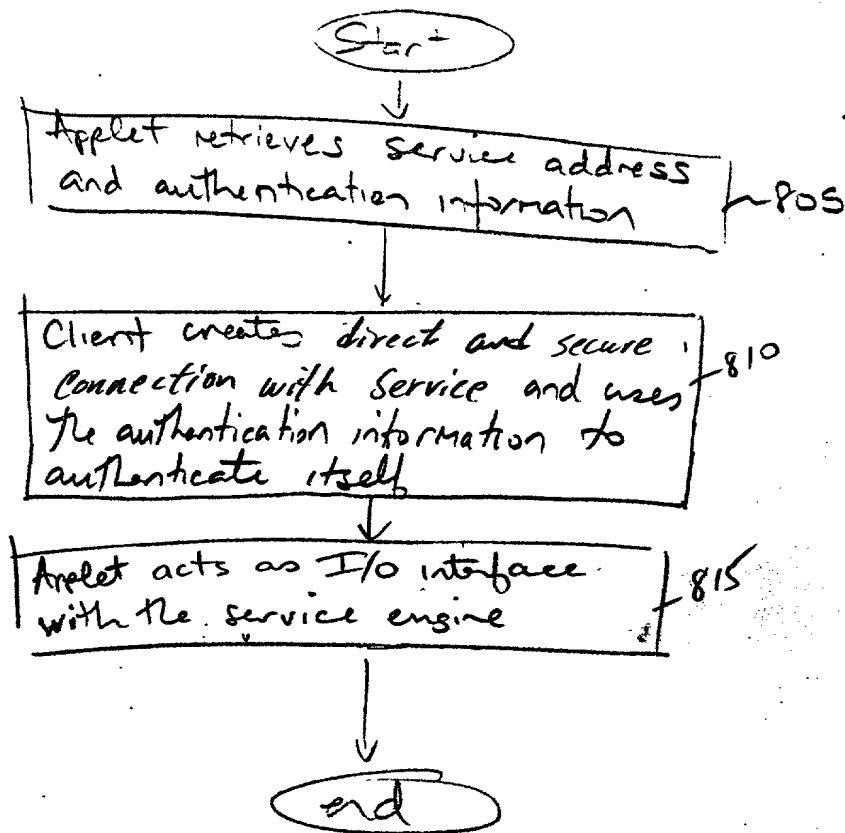


FIG. 8A (direct)

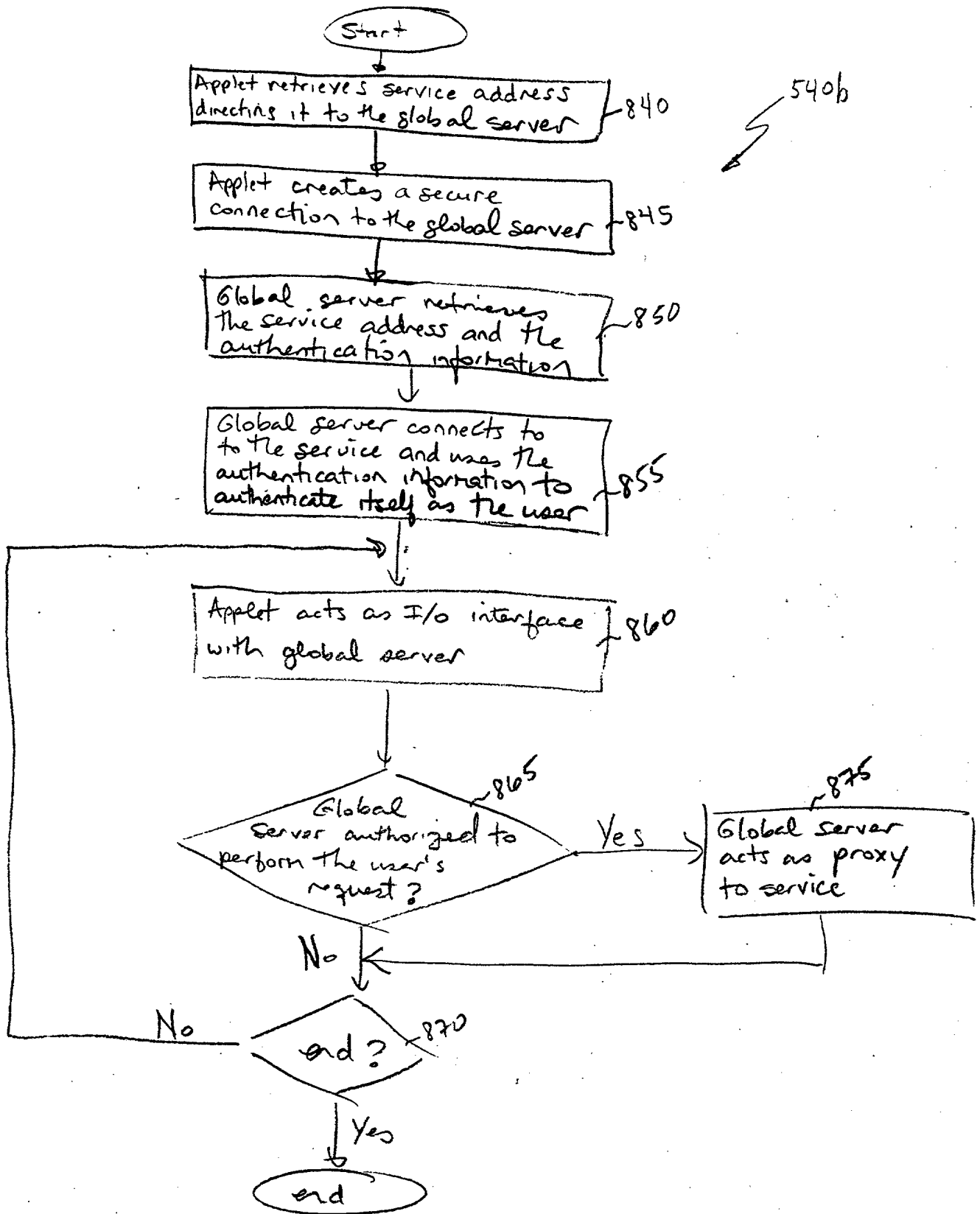
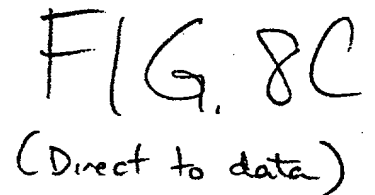


FIG. 8B (Proxy)

540c



(Direct to data)

ATTORNEY'S DOCKET NO.: 565

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "System and Method for Enabling Secure Access to Services in a Computer Network," the specification of which (check one):

☒ is attached hereto.
☐ was filed on _____ as U.S. Application No. _____
or PCT International Application No. _____
and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT International application, having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Claimed

_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
_____ (Number)	_____ (Country)	_____ (Day/Month/Year Filed)	<input type="checkbox"/> Yes	<input type="checkbox"/> No

I hereby claim the benefit under Title 35, United States Code §119(e) of any United States provisional application(s) listed below.

(Application Number)

(Filing Date)

(Application Number)

(Filing Date)

I hereby claim the benefit under Title 35, United States Code §120 of any United States application(s), or §365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

(Application Number)

(Filing Date)

(Status - patented, pending, abandoned)

(Application Number)

(Filing Date)

(Status - patented, pending, abandoned)

POWER OF ATTORNEY: I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

John S. Ferrell, Reg. No. 34,593; J. Eppa Hite, Reg. No. 30,266;
Leroy D. Maunu Reg. No. 35,274; Francis H. Lewis, Reg. No. 27,684;
Marc A. Sockol, Reg. No. P-40,823 and Gregory J. Koerner, Reg. No. 38,519

SEND ALL CORRESPONDENCE TO:

Marc A. Sockol
CARR, DEFILIPPO & FERRELL LLP
2225 East Bayshore Road, Suite 200
Palo Alto, CA 94303
TEL: (415) 812-3407
FAX: (415) 812-3444

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: Mark D. Riggins

Inventor's signature  Dated: 4-8-97

Residence 5818 Moraga Avenue, San Jose, CA 95123

Post Office Address same Citizenship USA

268010-0567980

Atty. Dkt.No. 565

Applicant: Mark D. Riggins
Serial or Patent No.: Unknown
Filed or Issued: Herewith
For: System and Method for Enabling Secure Access to Services in a Computer Network

VERIFIED STATEMENT (DECLARATION) CLAIMING
SMALL ENTITY STATUS
(37 CFR 1.9 (f) and 1.27 (c)) - SMALL BUSINESS CONCERN

I hereby declare that I am:

- ☐ the owner of the small business concern identified below:
☒ an official of the small business concern empowered to
act on behalf of the concern identified below:

NAME OF CONCERN RoamPage, Inc.
ADDRESS OF CONCERN 156 East Dana Street, Mountain View, CA 94041

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.2, and reproduced in 37 CFR 1.9 (d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, entitled "System and Method for Enabling Secure Access to Services in a Computer Network", by inventors Mark D. Riggins, described in

- ☒ the specification filed herewith.
☐ application serial no. _____, filed _____.
☐ patent no. _____, issued _____.

258040-0567880

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention is listed below* and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e). *NOTE: Separate verified statements are required from each named person, concern or organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

NAME _____

ADDRESS _____

☐ INDIVIDUAL ☐ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of the Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING Hong O. BuiTITLE OF PERSON Vice President of Product DevelopmentADDRESS 10250 Parkwood Drive, #4, Cupertino, CA 95014

SIGNATURE _____

DATE 4/7/97